

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION  
EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété  
Intellectuelle  
Bureau international



(43) Date de la publication internationale  
6 juin 2002 (06.06.2002)

PCT

(10) Numéro de publication internationale  
**WO 02/45031 A1**

(51) Classification internationale des brevets<sup>7</sup> : G07C 9/00

(71) Déposant (*pour MC seulement*) : SCHLUMBERGER MALCO, INC. [US/US]; 9800 Reisterstown, Owing Mills, MD 21117 (US).

(21) Numéro de la demande internationale :

PCT/IB01/02062

(72) Inventeurs; et

(22) Date de dépôt international :

1 novembre 2001 (01.11.2001)

(75) Inventeurs/Déposants (*pour US seulement*) : CUENOT, Serge [FR/FR]; 6, rue de la Combe, F-25320 Torpes (FR). MANDY, Damien [FR/FR]; 27, impasse Prays, F-25660 Fontain (FR).

(25) Langue de dépôt :

français

(74) Représentant commun : SCHLUMBERGER SYSTEMES; Service de la Propriété Intellectuelle, c/o Francis Fernandez, 50, avenue Jean Jaurès, F-92120 Montrouge (FR).

(30) Données relatives à la priorité :

00/15583 1 décembre 2000 (01.12.2000) FR

(81) États désignés (national) : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK,

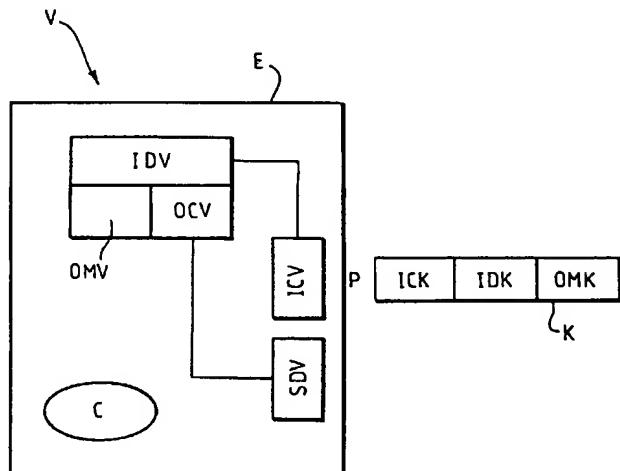
*[Suite sur la page suivante]*

(54) Title: DEVICE FOR SECURING ACCESS TO A CONTENT LOCATED INSIDE AN ENCLOSURE

(54) Titre : DISPOSITIF DE SECURISATION D'ACCÈS À UN CONTENU SITUÉ À L'INTÉRIEUR D'UNE ENCEINTE



**WO 02/45031 A1**



(57) Abstract: The enclosure (V) comprises a communication interface (ICV) with outside, means for processing (IDV, OCV) and means for transferring (OMV) the content and/or data concerning said content (C). The processing means (IDV, OCV) establish an authenticating function with homologous authenticating means (IDK) of a key (K) provided with at least an access right, via the communication interface (ICV) of the enclosure and an homologous communication interface (ICK) of the key (K). In case of positive authentication and positive verification of access right, the processing means of the enclosure (IDV, OCV) command the locking/unlocking means (SDV) to open the door (P). When the door is opened, the processing means of the enclosure (IDV, OCV) transfer the content and/or the content-related data derived from the transfer means of the enclosure (OMV) to the key of the enclosure, via the communication interface (ICV) of the enclosure and the homologous communication interface (ICK) of the key (K).

*[Suite sur la page suivante]*



LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX,  
MZ, NO, NZ, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK,  
SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA,  
ZW.

**Publiée :**

- avec rapport de recherche internationale
- entièrement sous forme électronique (sauf la présente page de couverture) et disponible sur demande auprès du Bureau international

(84) **États désignés (régional)** : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

*En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.*

---

(57) **Abrégé :** L'enceinte (V) comprend une interface de communication (ICV) avec l'extérieur de l'enceinte, des moyens de traitement (IDV, OCV) et des moyens de transfert (OMV) du contenu et/ou de données relatives audit contenu (C). Les moyens de traitement (IDV, OCV) établissent une fonction d'authentification avec des moyens d'authentification (IDK) homologues d'une clé (K) dotée d'au moins un droit d'accès, via l'interface de communication (ICV) de l'enceinte et une interface de communication (ICK) homologue de la clé (K). En cas d'authentification positive et de vérification positive du droit d'accès, les moyens de traitement de l'enceinte (IDV, OCV) commandent les moyens de verrouillage/déverrouillage (SDV) afin d'ouvrir la porte (P). En cas d'ouverture de la porte, les moyens de traitement de l'enceinte (IDV, OCV) transfèrent le contenu et/ou les données relatives audit contenu émanant des moyens de transfert de l'enceinte (OMV) vers la clé de l'enceinte, via l'interface de communication (ICV) de l'enceinte et l'interface de communication (ICK) homologue de la clé (K).

Dispositif de sécurisation d'accès à un contenu situé à l'intérieur d'une enceinte

La présente invention concerne la sécurisation d'accès à un contenu situé à l'intérieur d'une enceinte.

10 Elle trouve une application générale dans la sécurisation de biens, valeurs, services ou données, contenus dans une enceinte telle qu'un coffre ou boîte. Elle trouve une application particulière dans la sécurisation de valeurs contenues dans un horodateur, publiphone ou analogue.

On connaît déjà des dispositifs de sécurisation d'accès à un contenu situé à l'intérieur d'une enceinte.

20 Par exemple, dans la demande WO-A-93/12510, l'accès au contenu d'une borne d'un horodateur est sécurisé par un lecteur de carte à puce. Un intervenant introduit une carte à puce dans le lecteur. Après authentification de la carte à puce, et avant ouverture de la porte interdisant l'accès au 25 contenu de la borne, la carte à puce lit et enregistre les données d'un registre relatif au contenu de la borne. Après enregistrement, la carte à puce commande l'ouverture de la porte, afin de permettre le déroulement de l'intervention souhaitée.

30 Un tel dispositif de sécurisation d'accès n'est pas totalement satisfaisant.

En effet, le lecteur de carte à puce permet de reconnaître 35 (d'authentifier) l'intervenant avant l'ouverture de la porte, et d'assurer le transfert de données relatives au contenu vers la carte à puce. Mais, en raison du placement du lecteur de carte à puce à l'extérieur de la borne, et de la dissociation des étapes d'authentification de l'intervenant, du 40 transfert des données relatives au contenu de la borne, de

l'ouverture de la porte, et de l'accès au contenu de la borne, un tel lecteur ne permet pas de parer à la répudiation (c'est-à-dire la négation ou le démenti a posteriori) de l'accès au contenu de la borne de la part de l'intervenant.

5

La présente invention remédié à cet inconvénient.

Elle porte sur un dispositif de sécurisation d'accès à un contenu situé à l'intérieur d'une enceinte, ladite enceinte 10 étant du type comprenant une enveloppe apte à interdire l'accès audit contenu, une porte apte à permettre l'accès à l'intérieur de ladite enveloppe, et des moyens de verrouillage/déverrouillage de la porte.

15 Selon une définition générale de l'invention, l'enceinte comprend en outre une interface de communication avec l'extérieur de l'enceinte, des moyens de traitement et des moyens de transfert du contenu et/ou de données relatives audit contenu ;

20

lesdits moyens de traitement étant destinés à établir une fonction d'authentification avec des moyens d'authentification homologues d'une clé dotée d'au moins un droit d'accès, via l'interface de communication de l'enceinte et une 25 interface de communication homologue de la clé ;

en cas d'authentification positive et de vérification positive du droit d'accès, les moyens de traitement de l'enceinte étant aptes à commander les moyens de verrouillage/déverrouillage de la porte ; et

30 en cas d'ouverture de la porte, les moyens de traitement de l'enceinte étant destinés à transférer le contenu et/ou les données relatives audit contenu émanant des moyens de transfert de l'enceinte vers la clé, via l'interface de communication de l'enceinte et l'interface de communication homologue de la clé.

Ainsi, grâce au dispositif selon l'invention, l'intervenant qui est en charge d'effectuer le transfert du contenu ou de données relatives audit contenu de l'enceinte vers l'extérieur ne peut pas dissocier la nature de ses actions de la 5 clé qui lui a été confiée pour accéder audit contenu. Il en résulte que le dispositif de sécurisation selon l'invention offre un service de non répudiation à l'égard de l'accès au contenu de l'enceinte vis-à-vis de l'intervenant qui ouvre la porte de l'enceinte.

10 En d'autres termes, le dispositif selon l'invention offre le double avantage de se prémunir d'une éventuelle fraude (accès au contenu), réalisée par un individu malveillant (fonction de serrure) ainsi que de garantir que l'individu authentifié 15 réalisant la fonction de "collecte" du contenu ne puisse démentir un éventuel accès à ce contenu.

En pratique, les moyens de traitement de l'enceinte sont destinés à transférer le contenu et/ou les données relatives 20 audit contenu émanant des moyens de transfert de l'enceinte vers des moyens de mémorisation de la clé.

Ainsi, grâce à l'invention, les fonctions de serrure et de mémorisation sont cumulées avec la singularité de ne mémoriser 25 les informations qu'uniquement dans la clé qui a permis d'ouvrir la serrure (moyens de verrouillage/déverrouillage).

De préférence, la fonction d'authentification est du type actif.

30 Selon un autre aspect de l'invention, l'interface de communication de l'enceinte est du type appartenant au groupe formé par la technologie sans contact, avec contact ou mixte.

35 La présente invention a également pour objet une clé destinée à coopérer avec un dispositif de sécurisation d'accès à un contenu situé à l'intérieur d'une enceinte de type comprenant une enveloppe apte à interdire l'accès audit contenu, une porte apte à permettre l'accès à l'intérieur de ladite

enveloppe, et des moyens de verrouillage/déverrouillage de la porte.

Selon une autre caractéristique importante de l'invention, la  
5 clé est dotée d'au moins un droit d'accès et comprend une interface de communication destinée à communiquer avec une interface de communication homologue de l'enceinte, des moyens de traitement et des moyens de mémorisation ;

10 - lesdits moyens de traitement de la clé étant destinés à établir une fonction d'authentification avec les moyens d'authentification homologues des moyens de traitement de l'enceinte, via l'interface de communication de la clé et l'interface de communication homologue de l'enceinte, et

15 - en cas d'authentification positive et de vérification positive du droit d'accès, les moyens de verrouillage/déverrouillage étant destinés à être commandés afin d'ouvrir la porte ; et

20 - en cas d'ouverture de la porte de l'enceinte, les moyens de traitement de la clé étant destinés à transférer le contenu et/ou les données relatives audit contenu émanant des moyens de transfert de l'enceinte vers les moyens de mémorisation de la clé, via l'interface de communication de l'enceinte et l'interface de communication homologue de la clé.

En pratique, l'interface de communication de la clé est du type appartenant au groupe formé par la technologie sans contact, avec contact, ou mixte.

Selon un autre aspect de l'invention, des échanges d'informations sont réalisés entre l'interface de communication de l'enceinte et l'interface de communication de la clé pendant tout ou partie de la collecte jusqu'au verrouillage de la porte, ces échanges étant aptes à informer sur l'usage de la clé avec l'enceinte et/ou à inhiber/désinhiber le droit

d'accès de la clé et/ou les moyens d'authentification de la clé en fonction de l'usage de la clé avec l'enceinte.

Dans le cas d'un déroulement anormal du processus de collecte, tel que le non verrouillage de la porte, les moyens de traitement de l'enceinte sont aptes à inhiber le droit d'accès et/ou les moyens d'authentification de la clé.

Une telle inhibition du droit d'accès (tout ou partie des droits en cas de pluralité des droits d'accès) de la clé en cas de déroulement anormal du processus de collecte permet de limiter les opérations douteuses, volontaires ou non, de la part de l'intervenant qui, par exemple, retire sa clé de l'interface de communication de l'enceinte sans refermer et verrouiller la porte, afin de laisser l'enceinte ouverte et permettre ainsi de repasser ultérieurement prendre le contenu sans laisser de trace. Une telle opération a pour effet d'inhiber les droits de collecte de la clé qui ne peut plus alors servir pour les autres horodateurs et donc interdire la collecte dans lesdits autres horodateurs.

Dans le cas d'un déroulement normal du processus de collecte, les moyens de traitement de l'enceinte peuvent également inhiber le droit d'accès de la clé après authentification et vérification du droit d'accès et avant ouverture (déverrouillage) de la porte tandis que, après fermeture (verrouillage) de la porte, les moyens de traitement de l'enceinte sont destinés à désinhiber ledit droit d'accès de la clé.

L'inhibition/désinhibition des droits d'accès de la clé, notamment en relation avec l'ouverture/fermeture de la porte permet à un tiers, administrateur de la clé par exemple, de contrôler a posteriori l'usage de la clé par un intervenant choisi.

D'autres caractéristiques et avantages de l'invention apparaîtront à la lumière de la description détaillée ci-après et des dessins dans lesquels :

- la figure 1 illustre schématiquement les moyens constitutifs du dispositif de sécurisation d'accès à un contenu selon l'invention ; et

5 - la figure 2 est un organigramme illustrant le fonctionnement du dispositif selon l'invention.

En référence à la figure 1, un contenu C est situé à l'intérieur d'une enceinte V comportant une enveloppe E apte à interdire l'accès audit contenu C.

Une porte P (de préférence unique) permet l'accès (de préférence unique) à l'intérieur de l'enveloppe E.

15 Des moyens de verrouillage/déverrouillage SDV sont associés à la porte P pour permettre l'ouverture et la fermeture sécurisées de la porte.

20 L'enceinte V est une enceinte close correspondant, par exemple, à une tirelire ou un coffre d'un horodateur, et le contenu C est représentatif de valeurs sous forme de pièces..

L'enceinte peut être également celle d'un distributeur de titres, d'un distributeur de boissons, etc.

25 Les moyens de verrouillage/déverrouillage SDV sont commandés par des moyens de traitement et de commande OCV. Les moyens de verrouillage/déverrouillage peuvent être du type mécanique, logique ou analogique. Par exemple, les moyens de traitement et de commande OCV sont du type microprocesseur ou microcontrôleur.

35 De préférence, une mémoire OMV mémorise des données relatives au suivi du contenu C. Cette mémoire OMV est notamment utile pour contenir des données relatives aux transactions réalisées sur un horodateur.

Les données contenues dans cette mémoire peuvent être transférées dans une clé que l'on décrira plus en détail ci-après.

5 Par exemple, la mémoire OMV est du type EEPROM.

En variante, cette mémoire OMV peut être remplacée par un moyen de transfert de données et/ou de contenu.

10 Selon l'invention, l'enceinte V comprend en outre une interface de communication ICV avec l'extérieur de l'enceinte.

15 L'interface de communication ICV de l'enceinte appartient au groupe formé par la technologie sans contact, avec contact ou mixte.

20 Par exemple, l'interface de communication de l'enceinte est sans contact électrique, dit de proximité, correspondant à un échange de données avec une clé située à une distance de l'ordre de quelques millimètres.

25 La fonction d'authentification est par exemple du type actif. Elle comprend un échange de données entre la clé et l'enceinte selon un protocole de communication comprenant des communications cryptées et/ou bruitées.

30 Le chiffrement/déchiffrement des communications utilisent par exemple des fonctions de cryptographie classiques de type triple DES (pour "DATA ENCRYPTION SYSTEM").

35 Des moyens de traitement de l'enceinte IDV sont aptes à établir une fonction d'authentification avec des moyens d'authentification homologues de la clé K, via l'interface de communication ICV d'enceinte et l'interface de communication ICK homologue de la clé K.

De son côté, la clé K comprend une interface de communication ICK apte à communiquer avec l'interface de communication ICV

homologue de l'enceinte. De plus, la clé K est dotée d'au moins un droit d'accès. Par exemple, le droit d'accès est un droit de collecte du contenu. D'autres droits d'accès peuvent être utilisés.

5

Des moyens de traitement de la clé IDK sont aptes à piloter l'échange des données via l'interface de communication ICK. Ces moyens de traitement IDK sont en outre capables de piloter l'écriture/lecture dans les moyens de mémorisation

10

OMK. Les moyens de mémorisation OMK peuvent par exemple mémoriser des données relatives au suivi du contenu C.

Par exemple, les moyens de traitement de la clé sont du type microprocesseur ou microcontrôleur.

15

La mémoire OMK est par exemple du type EEPROM.

20

La clé K peut être du format d'une carte à mémoire ou analogue. Elle est réalisée en technologie avec ou sans contact ou bien encore mixte.

L'alimentation en énergie est fournie prioritairement par l'enceinte mais elle peut être fournie par la clé (alimentation interne de la clé) en cas de panne l'enceinte.

25

En référence à la figure 2, le fonctionnement du dispositif de sécurisation selon l'invention dans le cadre d'une collecte du contenu C et/ou de données relatives audit contenu est le suivant.

30

Selon l'étape E1, l'intervenant présente sa clé K devant l'interface de communication ICV de l'enceinte V.

35

Selon l'étape E2, la fonction d'authentification de la clé K est mise en place à l'aide des moyens de traitement IDV de l'enceinte et des moyens de traitement IDK de la clé K.

En cas d'authentification positive et de vérification positive du droit d'accès (étape E3), la collecte peut

commencer selon un protocole prédéterminé comprenant des échanges entre l'interface de communication de la clé et l'interface de communication de l'enceinte jusqu'au moment du verrouillage de la porte.

5

Avantageusement, ces échanges sont aptes à informer sur l'usage de la clé avec l'enceinte, et/ou à inhiber/désinhiber le droit d'accès et/ou les moyens d'authentification de la clé en fonction de l'usage de la clé avec l'enceinte.

10

Dans le cas d'un déroulement anormal du processus de collecte, tel que le non verrouillage de la porte, les moyens de traitement de l'enceinte peuvent inhiber le droit d'accès et/ou les moyens d'authentification de la clé.

15

Dans le cas d'un déroulement anormal du processus de collecte, les moyens de traitement de l'enceinte peuvent également inhiber/désinhiber le droit d'accès et/ou les moyens d'authentification de la clé. En pratique, cette inhibition peut intervenir avant l'ouverture de la porte, et être annulée par une désinhibition réciproque en cas de fermeture normale de la porte.

25

Selon l'étape E4, les moyens de traitement et de commande de l'enceinte OCV commandent le déverrouillage (ouverture) de la porte P.

30

En cas d'ouverture de la porte (étape E5), les moyens de traitement de l'enceinte IDV et/ou OCV sont aptes à transférer le contenu C et/ou les données relatives audit contenu C émanant des moyens de transfert (mémorisation) de l'enceinte OMV vers la clé K de l'enceinte, via l'interface de communication ICV de l'enceinte et l'interface de communication ICK homologue de la clé K.

35

En pratique, le transfert du contenu C émanant des moyens de transfert de l'enceinte OMV est effectué dans les moyens de mémorisation homologues OMK de la clé K.

Les données ainsi transférées sont préalablement introduites dans les moyens de transfert OMV par un système interne qui régit l'enceinte.

5 Après le transfert des données, l'utilisateur retire sa clé de l'interface de communication de l'enceinte pendant ou après le verrouillage de la porte P.

De préférence, les communications entre l'enceinte et la clé 10 sont réalisées sans contact électrique, c'est-à-dire par induction. Une telle fonction d'introduction de la clé dans la serrure par proximité confère une protection supplémentaire vis-à-vis de l'espionnage frauduleux dans la mesure où l'induction est réalisée à l'intérieur de l'enceinte.

15 Les communications entre l'enceinte et la clé peuvent être cryptées et/ou bruitées par des codes de cession (codes générés de façon aléatoire, valides uniquement pendant une ouverture tant que la clé est présente dans l'interface de 20 communication de l'enceinte ICV).

Ainsi, non seulement lors de l'ouverture de la porte permettant l'accès au contenu de l'enceinte mais également tout le temps de la collecte, s'opèrent des échanges d'informations 25 entre l'interface de communication de l'enceinte et l'interface de communication de la clé.

Il en résulte qu'il est possible de modifier les droits 30 d'accès de la clé en cas de déroulement anormal du processus de collecte.

Ainsi par exemple, le droit de collecte de la clé peut être inhibé si la clé est retirée et que la porte n'est pas refermée (autorisant donc un accès libre au contenu de 35 l'enceinte).

Le droit d'accès de la clé étant inhibé, il n'est alors plus possible à l'intervenant de poursuivre sa tournée sur

d'autres horodateurs puisqu'il ne pourra alors plus déverrouiller lesdits horodateurs.

L'inhibition du droit de collecte permet par ailleurs de suivre la trace de l'intervenant puisque les horodateurs conservent les codes d'authentification des clés qui leur sont présentées.

Par exemple, la validation ou non de la fonction de commande d'ouverture de la porte est réalisée à l'issue d'une comparaison d'états internes entre la clé et l'enceinte.

Selon l'étape E7, après fermeture normale (verrouillage) de la porte, le ou les droits d'accès de la clé K peuvent être désinhibés (passage d'un drapeau du microprocesseur de la clé à l'état bas correspondant à la désinhibition de la clé) selon un protocole choisi entre la clé et l'enceinte.

Une telle information sur l'usage de la clé accompagnée ou non de l'inhibition/désinhibition du ou des droits d'accès de la clé, notamment en synchronisation avec l'ouverture/fermeture de la porte permet de tracer des éventuelles opérations malveillantes d'un intervenant.

La présente invention trouve une application dans la collecte de l'argent au sein d'un distributeur quelconque (horodateur, distributeur de titres, distributeur de boissons, etc.). Elle peut également s'appliquer au contrôle d'accès ou de rondes en attestant dans la clé électronique que les différents passages ont été faits (mémorisation des données telles que la date, l'heure, etc.).

Revendications

1. Dispositif de sécurisation d'accès à un contenu (C)  
5 situé à l'intérieur d'une enceinte (V),

ladite enceinte étant du type comprenant une enveloppe (E) apte à interdire l'accès audit contenu, une porte (P) apte à permettre l'accès à l'intérieur de ladite enveloppe (E), et  
10 des moyens de verrouillage/déverrouillage (SDV) de la porte (P),

15 caractérisé en ce que l'enceinte comprend en outre une interface de communication (ICV) avec l'extérieur de l'enceinte, des moyens de traitement (IDV, OCV) et des moyens de transfert (OMV) du contenu et/ou de données relatives audit contenu (C),

20 lesdits moyens de traitement (IDV, OCV) étant destinés à établir une fonction d'authentification avec des moyens d'authentification (IDK) homologues d'une clé (K) dotée d'au moins un droit d'accès, via l'interface de communication (ICV) de l'enceinte et une interface de communication (ICK) homologue de la clé (K),  
25

en cas d'authentification positive et de vérification positive du droit d'accès, les moyens de traitement de l'enceinte (IDV, OCV) étant aptes à commander les moyens de verrouillage/déverrouillage (SDV) afin d'ouvrir la porte (P),  
30 et

en cas d'ouverture de la porte, les moyens de traitement de l'enceinte (IDV, OCV) étant destinés à transférer le contenu et/ou les données relatives audit contenu émanant des moyens de transfert de l'enceinte (OMV) vers la clé de l'enceinte, via l'interface de communication (ICV) de l'enceinte et l'interface de communication (ICK) homologue de la clé (K).

2. Dispositif selon la revendication 1, caractérisé en ce que les moyens de traitement de l'enceinte (IDV, OCV) sont destinés à transférer le contenu et/ou les données relatives audit contenu émanant des moyens de transfert de l'enceinte (OMV) vers des moyens de mémorisation (OMK) homologues de la clé.

3. Dispositif selon la revendication 1 ou la revendication 2, caractérisé en ce que la fonction d'authentification est active.

4. Dispositif selon l'une des revendications précédentes, caractérisé en ce que l'interface de communication (ICV) de l'enceinte est du type appartenant au groupe formé par la technologie sans contact, avec contact ou mixte.

5. Dispositif selon l'une des revendications 1 à 4, caractérisé en ce que des échanges d'informations sont réalisés entre l'interface de communication de l'enceinte et l'interface de communication de la clé jusqu'au moment du verrouillage de la porte, ces échanges étant aptes à informer sur l'usage de la clé avec l'enceinte et/ou à inhiber/désinhiber le droit d'accès de la clé et/ou les moyens d'authentification de la clé en fonction de l'usage de la clé avec l'enceinte.

6. Dispositif selon la revendication 5, caractérisé en ce que dans le cas d'un déroulement anormal du processus de collecte, les moyens de traitement de l'enceinte sont aptes à inhiber le droit d'accès et/ou des moyens d'authentification de la clé.

7. Dispositif selon la revendication 5, caractérisé en ce qu'après vérification du droit d'accès et avant ouverture de la porte, les moyens de traitement de l'enceinte (IDV, OCV) sont aptes à inhiber le droits d'accès de la clé tandis qu'après fermeture normale de la porte, les moyens de traitement de l'enceinte (IDV, OCV) sont aptes à désinhiber le droit d'accès de la clé.

8. Clé destinée à coopérer avec un dispositif de sécurisation d'accès à un contenu (C) situé à l'intérieur d'une enceinte (V) du type comprenant une enveloppe (E) apte à interdire l'accès audit contenu, une porte (P) apte à permettre l'accès à l'intérieur de ladite enveloppe (E), des moyens de traitement (IDV) et des moyens de verrouillage/déverrouillage (SDV) de la porte (P),

10 caractérisée en ce que la clé (K) est dotée d'au moins un droit d'accès et comprend une interface de communication (ICK) destinée à communiquer avec une interface de communication (ICV) homologue de l'enceinte, des moyens de traitement (IDK) et des moyens de mémorisation (OMK),

15 lesdits moyens de traitement (IDK) de la clé étant destinés à établir une fonction d'authentification avec des moyens d'authentification (IDV) homologues des moyens de traitement de l'enceinte, via l'interface de communication (ICK) de la clé (K) et l'interface de communication (ICV) homologue de l'enceinte (V),

20 en cas d'authentification positive et de vérification positive du droit d'accès, les moyens de verrouillage/déverrouillage étant destinés à être commandés afin d'ouvrir la porte (P) ; et

25 en cas d'ouverture de la porte de l'enceinte, les moyens de traitement (IDK) de la clé étant destinés à transférer le contenu et/ou les données relatives audit contenu émanant des moyens de transfert de l'enceinte (OMV) vers les moyens de mémorisation de la clé, via l'interface de communication (ICV) de l'enceinte et l'interface de communication (ICK) homologue de la clé (K).

30 35 9. Clé selon la revendication 8, caractérisée en ce que des échanges d'informations sont réalisés entre l'interface de communication de l'enceinte et l'interface de communication de la clé pendant tout ou partie de la collecte jusqu'au

moment du verrouillage de la porte, ces échanges étant aptes à informer sur l'usage de la clé et/ou à inhiber/désinhiber le droit d'accès de la clé et/ou les moyens d'authentification de la clé en fonction de l'usage de la clé avec l'enceinte.

5           10. Clé selon la revendication 9, caractérisée en ce qu'en cas de déroulement anormal de la collecte, le droit d'accès et/ou les moyens d'authentification de la clé, sont susceptibles d'être inhibés.

15           11. Clé selon la revendication 10, caractérisée en ce qu'après authentification de la clé et vérification du droit d'accès et avant déverrouillage de la porte, les moyens de traitement de l'enceinte (IDV, OCV) sont destinés à inhiber le droit d'accès de la clé tandis qu'après verrouillage normal de la porte (P), les moyens de traitement (IDV, OCV) de l'enceinte sont destinés à désinhiber le droit d'accès de la clé.

20           12. Clé selon la revendication 9, caractérisée en ce que la fonction d'authentification est active.

25           13. Clé selon l'une des revendications 9 à 12, caractérisée en ce que l'interface de communication (ICK) de la clé est du type appartenant au groupé formé par la technologie sans contact, avec contact, ou mixte.

30           14. Clé selon l'une des revendications 9 à 13, caractérisée en ce qu'elle est au format d'une carte à mémoire ou analogue.

1/2

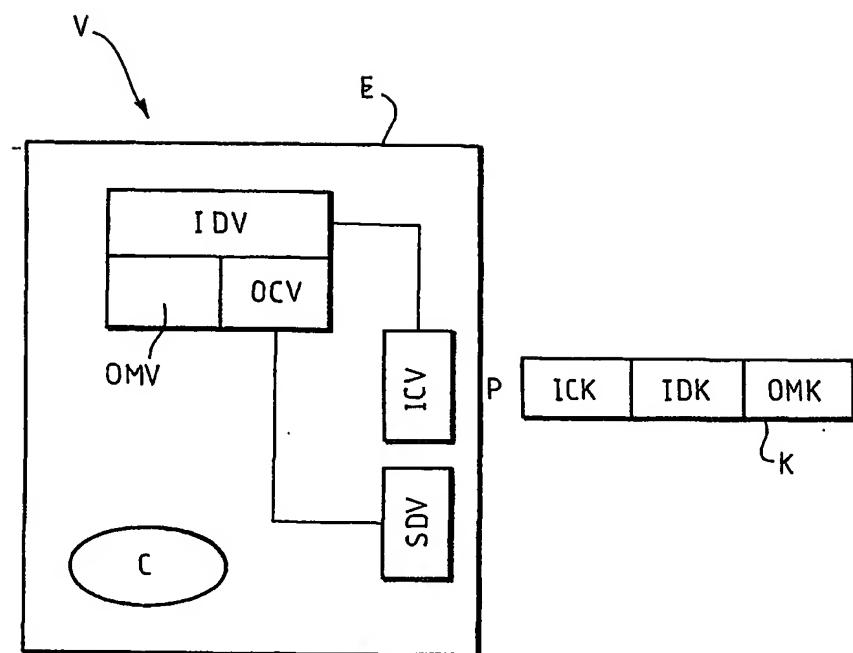


FIG.1

2/2

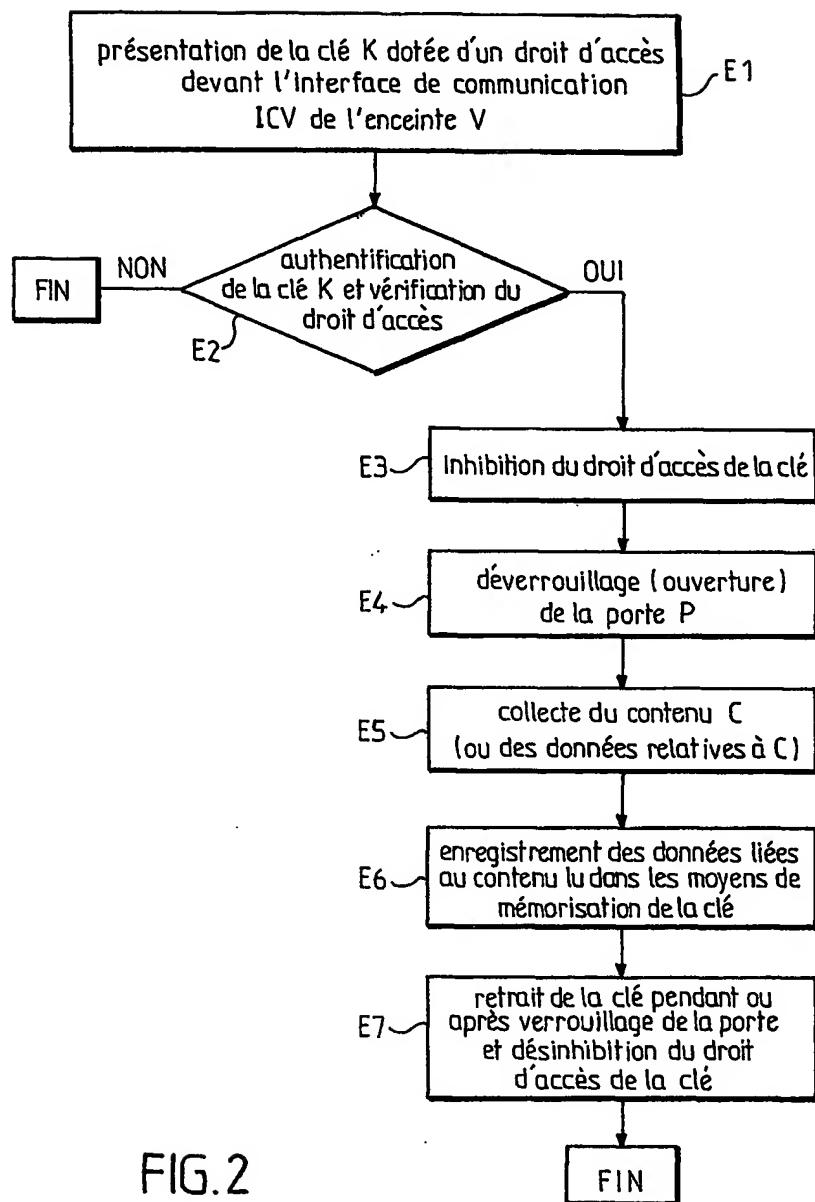


FIG.2

## INTERNATIONAL SEARCH REPORT

Inte  
al Application No  
PCT/IB 01/02062

**A. CLASSIFICATION OF SUBJECT MATTER**  
IPC 7 G07C9/00

According to International Patent Classification (IPC) or to both national classification and IPC

**B. FIELDS SEARCHED**

Minimum documentation searched (classification system followed by classification symbols)  
IPC 7 G07C E05B G07D G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the International search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 520 275 A (FOGLINO JEAN-JACQUES) 28 May 1996 (1996-05-28)	1-5, 8, 9, 12-14
Y	column 3, line 34 -column 5, line 8 figures 1,2 ---	6, 10
Y	US 5 745 044 A (TRENT DOUGLAS ET AL) 28 April 1998 (1998-04-28)	6, 10
A	claims 1,4; figures 1-4 ---	1, 8
A	GB 2 346 412 A (MARCONI COMM LTD) 9 August 2000 (2000-08-09) page 13, line 1 -page 14, line 20 figures 1,2 ---	1-4, 8, 12-14
A	US 5 415 264 A (MENOUD EDOUARD) 16 May 1995 (1995-05-16) column 6, line 15 - line 68 figures 1,3,4 ---	1-4, 8, 12-14
		-/-

Further documents are listed in the continuation of box C.

Patent family members are listed in annex.

\* Special categories of cited documents :

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier document but published on or after the International filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the International filing date but later than the priority date claimed

- "T" later document published after the International filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- "&" document member of the same patent family

Date of the actual completion of the International search

25 February 2002

Date of mailing of the International search report

04/03/2002

Name and mailing address of the ISA  
European Patent Office, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel: (+31-70) 340-2040, Tx. 31 651 epo nl.  
Fax: (+31-70) 340-3016

Authorized officer

Miltgen, E

## INTERNATIONAL SEARCH REPORT

Inte Application No  
PCT/IB 01/02062

## C(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 387 972 A (KLUESSENDORF AG) 19 September 1990 (1990-09-19) abstract; claims; figures ---	1,8
A	FR 2 738 436 A (NOVELLA CARMELO) 7 March 1997 (1997-03-07) ---	

## INTERNATIONAL SEARCH REPORT

Information on patent family members

Inte  
al Application No

PCT/IB 01/02062

Patent document cited in search report	Publication date		Patent family member(s)	Publication date
US 5520275	A 28-05-1996	FR DE DE EP ES WO JP	2685113 A1 69231470 D1 69231470 T2 0617819 A1 2152247 T3 9312510 A1 7507647 T	18-06-1993 26-10-2000 23-05-2001 05-10-1994 01-02-2001 24-06-1993 24-08-1995
US 5745044	A 28-04-1998	US CA EP JP US WO US AT CA DE DE DK EP WO	5140317 A 2133743 A1 0635182 A1 7505988 T 6005487 A 9321712 A1 5541581 A 173315 T 2082649 A1 69130477 D1 69130477 T2 527886 T3 0527886 A1 9118169 A1	18-08-1992 28-10-1993 25-01-1995 29-06-1995 21-12-1999 28-10-1993 30-07-1996 15-11-1998 12-11-1991 17-12-1998 12-05-1999 26-07-1999 24-02-1993 28-11-1991
GB 2346412	A 09-08-2000	GB EP ZA	2342115 A 0990753 A2 9906217 A	05-04-2000 05-04-2000 11-04-2000
US 5415264	A 16-05-1995	AT DE DK EP ES FI NO	155599 T 59306912 D1 570692 T3 0570692 A1 2106913 T3 932226 A 931775 A	15-08-1997 21-08-1997 29-12-1997 24-11-1993 16-11-1997 23-11-1993 23-11-1993
EP 0387972	A 19-09-1990	DE AT DD DE DK EP ES	3909323 A1 100955 T 292985 A5 59004375 D1 387972 T3 0387972 A1 2049409 T3	20-09-1990 15-02-1994 14-08-1991 10-03-1994 11-04-1994 19-09-1990 16-04-1994
FR 2738436	A 07-03-1997	FR FR	2738435 A1 2738436 A1	07-03-1997 07-03-1997

## RAPPORT DE RECHERCHE INTERNATIONALE

Dem internationale No  
PCT/IB 01/02062

**A. CLASSEMENT DE L'OBJET DE LA DEMANDE**  
CIB 7 G07C9/00

Selon la classification Internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

**B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE**

Documentation minimale consultée (système de classification suivi des symboles de classement)  
CIB 7 G07C E05B G07D G07F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

EPO-Internal, WPI Data

**C. DOCUMENTS CONSIDERES COMME PERTINENTS**

Catégorie	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	US 5 520 275 A (FOGLINO JEAN-JACQUES) 28 mai 1996 (1996-05-28)	1-5, 8, 9, 12-14
Y	colonne 3, ligne 34 -colonne 5, ligne 8 figures 1,2 ---	6, 10
Y	US 5 745 044 A (TRENT DOUGLAS ET AL) 28 avril 1998 (1998-04-28)	6, 10
A	revendications 1,4; figures 1-4 ---	1, 8
A	GB 2 346 412 A (MARCONI COMM LTD) 9 août 2000 (2000-08-09) page 13, ligne 1 -page 14, ligne 20 figures 1,2 ---	1-4, 8, 12-14
A	US 5 415 264 A (MENOUD EDOUARD) 16 mai 1995 (1995-05-16) colonne 6, ligne 15 - ligne 68 figures 1,3,4 ---	1-4, 8, 12-14
	-/-	

Voir la suite du cadre C pour la fin de la liste des documents

Les documents de familles de brevets sont indiqués en annexe

\* Catégories spéciales de documents cités:

- \*A\* document définissant l'état général de la technique, non considéré comme particulièrement pertinent
- \*E\* document antérieur, mais publié à la date de dépôt international ou après cette date
- \*L\* document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
- \*O\* document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
- \*P\* document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

- \*T\* document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention
- \*X\* document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
- \*Y\* document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier
- \*&\* document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée

25 février 2002

Date d'expédition du présent rapport de recherche internationale

04/03/2002

Nom et adresse postale de l'administration chargée de la recherche internationale  
Office Européen des Brevets, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax: (+31-70) 340-3016

Fonctionnaire autorisé

Miltgen, E

## RAPPORT DE RECHERCHE INTERNATIONALE

Dem	internationale No
PCT/IB 01/02062	

## C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	EP 0 387 972 A (KLUESSENDORF AG) 19 septembre 1990 (1990-09-19) abrégé; revendications; figures -----	1,8
A	FR 2 738 436 A (NOVELLA CARMELO) 7 mars 1997 (1997-03-07) -----	

**RAPPORT DE RECHERCHE INTERNATIONALE**

Renseignements relatifs aux membres de familles de brevets

Demande internationale No

PCT/IB 01/02062

Document brevet cité au rapport de recherche		Date de publication		Membre(s) de la famille de brevet(s)	Date de publication
US 5520275	A	28-05-1996	FR DE DE EP ES WO JP	2685113 A1 69231470 D1 69231470 T2 0617819 A1 2152247 T3 9312510 A1 7507647 T	18-06-1993 26-10-2000 23-05-2001 05-10-1994 01-02-2001 24-06-1993 24-08-1995
US 5745044	A	28-04-1998	US CA EP JP US WO US AT CA DE DE DK EP WO	5140317 A 2133743 A1 0635182 A1 7505988 T 6005487 A 9321712 A1 5541581 A 173315 T 2082649 A1 69130477 D1 69130477 T2 527886 T3 0527886 A1 9118169 A1	18-08-1992 28-10-1993 25-01-1995 29-06-1995 21-12-1999 28-10-1993 30-07-1996 15-11-1998 12-11-1991 17-12-1998 12-05-1999 26-07-1999 24-02-1993 28-11-1991
GB 2346412	A	09-08-2000	GB EP ZA	2342115 A 0990753 A2 9906217 A	05-04-2000 05-04-2000 11-04-2000
US 5415264	A	16-05-1995	AT DE DK EP ES FI NO	155599 T 59306912 D1 570692 T3 0570692 A1 2106913 T3 932226 A 931775 A	15-08-1997 21-08-1997 29-12-1997 24-11-1993 16-11-1997 23-11-1993 23-11-1993
EP 0387972	A	19-09-1990	DE AT DD DE DK EP ES	3909323 A1 100955 T 292985 A5 59004375 D1 387972 T3 0387972 A1 2049409 T3	20-09-1990 15-02-1994 14-08-1991 10-03-1994 11-04-1994 19-09-1990 16-04-1994
FR 2738436	A	07-03-1997	FR FR	2738435 A1 2738436 A1	07-03-1997 07-03-1997